第 6 回有限体理論とその擬似乱数系列生成への応用ワークショップ開催報告

開催方法：オンライン（WebEX）
開催期間：2020 年 9 月 28 日（月）～29 日（火）

実行委員長　小寺雄太（岡山大学）

2020 年 9 月 28 日（月）から 29 日（火）の 2 日間、第 6 回有限体理論とその擬似乱数系列生成への応用ワークショップ（FFTPRSWS 2020）をオンラインにて開催しました。このワークショップは、情報理論とその応用シンポジウム（SITA）あるいは、International Symposium on Information Theory and Its Applications（ISITA)などにおいて、日頃より有限体理論とその擬似乱数系列生成への応用に関連する研究の成果発表をしている研究者、またそのようなテーマに興味を持っている研究者が一堂に会し、日々の研究活動の中で得られた成果の報告をはじめ、疑問に思っている事柄、あるいは個人的な興味から深く掘り下げているテーマなどを、十分な時間をかけてお互いに紹介、共有し、密な議論を展開するための場を提供することを意図したワークショップです。

第 1 回目は 2015 年 8 月に群馬県吾妻群草津町（草津温泉）で開催され、その後、2016 年 9 月に大分県由布市（湯布院温泉)、2017 年 10 月に北海道旭川市（旭川市民文化会館)、2018 年 8 月に山口県萩市（萩・明倫館)、2019 年 9 月に福岡県福岡市（九州工業大学サテライト福岡天神）にて開催されてきました。

第 6 回目となる FFTPRSWS 2020 は、世界的に流行した新型コロナウイルス感染症（COVID-19）へ配慮し、全面オンラインでの開催となりました。

私事ではございますが、2020 年度 3 月に博士課程を修了し、岡山大学にて研究者としての第一歩を踏み出した年に、本ワークショップの実行委員長を仰せつかり、多くのことを経験することができました。このような場をご提供くださった皆様にこの場をお借りして感謝いたします。

今回のワークショップは全面オンラインで開催ということもあり、遠方のため現地開催ではご参加が容易ではなかった方をはじめ、これまでご参加いただいたことのなかった方など過去最多となる参加者の皆様をむかえてのワークショップ開催となりました。

さて、肝心のワークショップですが、21 名（一般 16 名、学生 5 名）の参加があり、7 件の一般公演の発表がありました。いずれの発表においても、熱心かつ有意義なディスカッションが行われました。

発表者と発表題目は以下の通りです（敬称略)。

一般公演 1）小薗 元（九州工業大学）
「整数上のロジスティック写像における定義域に関する一考察」

一般公演 2）多田羅友也（岡山大学）
「Cascaded NTU 系列の線形複雑度に関する考察」

一般公演 3）高谷 つぐみ（岡山大学）

「暗号向け乱数生成における非線形フィルタの設計に関する考察」

一般公演 4）村岡 英之（東芝情報システム株式会社）

「乱数生成器に対する統計検定フレームワークに関する考察」

一般公演 5）佐藤 陵一（岡山大学）

「リングオシレータを用いた小規模な物理乱数生成回路の設計および乱数性評価」

一般公演 6）小嶋 徹也（東京工業高等専門学校）

「有限体上のアダマール型行列と離散フーリエ変換」

一般公演 7）宮崎 武（北九州市立大学）

「幾つかの系列に対する周期探索法と，素体上のロジスティック写像の逆写像演算について」

初めてご参加いただいた方や学生を交えた忌憚のない活発な議論や交流の場を設けることができた有意義なワークショップとなりました。

なお、今回でも前回と同様に予稿集を発行し、参加者各位へはパスワード付き zip ファイルとしてお渡し、ワークショップ内でパスワードをお伝えすることで配布いたしました。

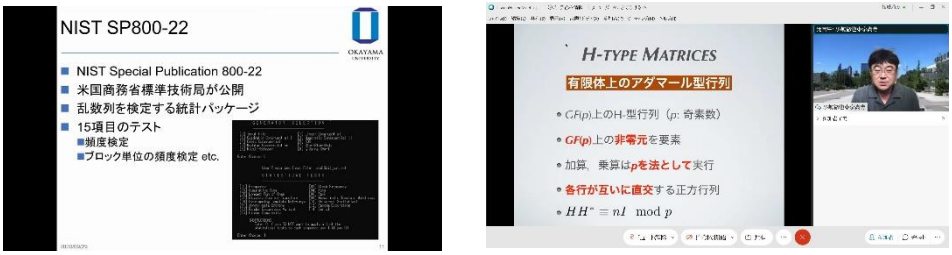

図 1. 発表の様子